(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11355265 A**

(43) Date of publication of application: **24 . 12 . 99**

(51) Int. Cl **H04L 9/14**
G06F 13/00
G06F 13/00
H04H 1/00
H04L 9/32
H04L 29/08
H04N 7/167
// G06F 13/38
H04L 12/28

(21) Application number: **10162667**

(22) Date of filing: **10 . 06 . 98**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor: **NISHIMURA TAKUYA**
IIZUKA HIROYUKI
YAMADA MASAZUMI
GOTO SHOICHI
TAKECHI HIDEAKI

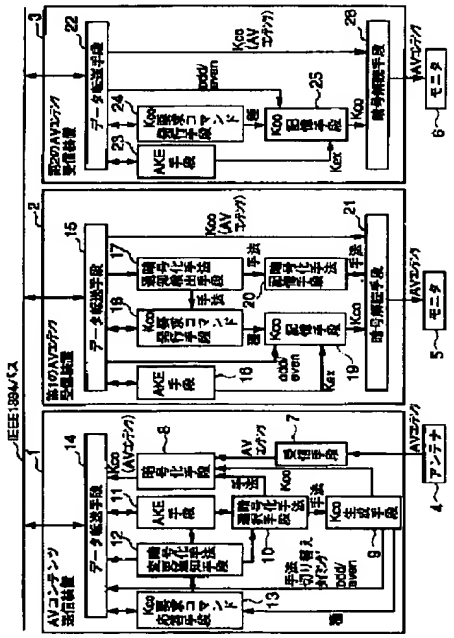
(54) **METHOD FOR AV CONTENTS TRANSMISSION AND AV CONTENTS RECEPTION, DEVICE FOR AV CONTENTS TRANSMISSION AND AV CONTENTS RECEPTION AND MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an AV contents transmission method that an AV contents receiver, which cannot use a first enciphering method when an AV contents transmitter is receiving the AV contents enciphered by the first enciphering method, can decode its AV contents.

SOLUTION: If there is a authentication demand from a second contents receiver which cannot use an extended enciphering method while an AV contents transmitter 1 is transmitting AV contents enciphered by the extended enciphering method by using an IEEE 1394 bus, then after the authentication is successful, the AV contents transmitter 1 enciphers the AV contents by a basic enciphering method, which a second AV contents receiver 3 making the authentication demand can use, and transmits them.

COPYRIGHT: (C)1999,JPO



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－355265

(43)公開日　平成11年(1999)12月24日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６４１
Ｇ０６Ｆ	13/00	３５１	Ｇ０６Ｆ	13/00	３５１Ａ
		３５７			３５７Ａ
Ｈ０４Ｈ	1/00		Ｈ０４Ｈ	1/00	Ｆ
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	13/38	３５０

審査請求　未請求　請求項の数20　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平10－162667

(22)出願日　平成10年(1998)６月10日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　西村　拓也
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

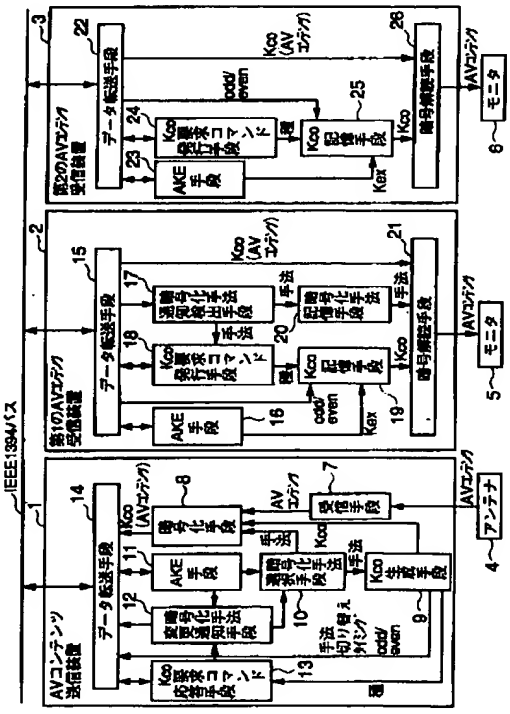
最終頁に続く

(54)【発明の名称】　ＡＶコンテンツ送信方法、ＡＶコンテンツ受信方法、ＡＶコンテンツ送信装置、ＡＶコンテンツ受信装置および媒体

(57)【要約】

【課題】ＡＶコンテンツ送信装置が拡張暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その拡張暗号化手法を使用することができないＡＶコンテンツ受信装置はそのＡＶコンテンツを解読することができない。

【解決手段】ＡＶコンテンツ送信装置１がＩＥＥＥ１３９４バスを利用して拡張暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その拡張暗号化手法を使用することができない第２のＡＶコンテンツ受信装置３から認証要求があると、その認証が成功した後、ＡＶコンテンツ送信装置１は、その認証要求をした第２のＡＶコンテンツ受信装置３が使用することができる基本暗号化手法でＡＶコンテンツを暗号化して送信する。



【特許請求の範囲】

【請求項１】ＡＶコンテンツ送信装置が伝送路を利用して第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、
その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、
その認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法で前記ＡＶコンテンツを暗号化して送信することを特徴とするＡＶコンテンツ送信方法。

【請求項２】前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、
その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知することを特徴とする請求項１記載のＡＶコンテンツ送信方法。

【請求項３】前記暗号化手法の切り替えを、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項２記載のＡＶコンテンツ送信方法。

【請求項４】前記切り替えた後の前記第２の暗号化手法がどのような暗号化手法であるのかという情報を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項３記載のＡＶコンテンツ送信方法。

【請求項５】前記切り替えた後の前記第２の暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とする請求項３記載のＡＶコンテンツ送信方法。

【請求項６】前記暗号化手法の切り替えのタイミングを、前記認証要求がある前に使用していた前記第１の暗号化手法での暗号化鍵の更新のタイミングとすることを特徴とする請求項１記載のＡＶコンテンツ送信方法。

【請求項７】少なくとも前記別のＡＶコンテンツ受信装置に、前記暗号化手法が前記第２の暗号化手法に切り替わることを通知するとともに、その暗号化手法の切り替えのタイミングの情報を送信することを特徴とする請求項２記載のＡＶコンテンツ送信方法。

【請求項８】前記ＡＶコンテンツ送信装置が前記認証要求をしたＡＶコンテンツ受信装置を記憶し、
そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなった場合、
前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とする請求項１記載のＡＶコンテンツ送信方法。

【請求項９】前記ＡＶコンテンツ送信装置が、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、
前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とする請求項１記載のＡＶコンテンツ送信方法。

【請求項１０】請求項１から９のいずれかに記載のＡＶコンテンツ送信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体。

【請求項１１】請求項１から９のいずれかに記載のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツを受信し、
そのＡＶコンテンツが暗号化されたさいに使用された暗号化手法に基づくとともに、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読することを特徴とするＡＶコンテンツ受信方法。

【請求項１２】請求項１から９のいずれかに記載のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、
その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、
前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記暗号化手法の切り替えに関する情報に含まれていないものを送信するように要求することを特徴とする請求項１１記載のＡＶコンテンツ受信方法。

【請求項１３】請求項１１または１２記載のＡＶコンテンツ受信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体。

【請求項１４】送信しようとするＡＶコンテンツを暗号化するさいの暗号化手法を選択する暗号化手法選択手段と、
その暗号化手法選択手段によって選択された暗号化手法に対応した、ＡＶコンテンツを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、
ＡＶコンテンツを入力するとともに、前記暗号化鍵生成

手段からの前記暗号化鍵を入力し、その暗号化鍵を利用して、前記ＡＶコンテンツを暗号化する暗号化手段と、ＡＶコンテンツ受信装置との間で認証・鍵交換を行う送信側認証・鍵交換手段とを備え、
ＡＶコンテンツ送信装置が、前記暗号化手法選択手段によって選択された第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、
その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、前記送信側認証・鍵交換手段は、その認証要求をしたＡＶコンテンツ受信装置との間で認証を行い、
前記暗号化手法選択手段は、暗号化手法を、前記認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法に切り替えることを特徴とするＡＶコンテンツ送信装置。
【請求項１５】前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、
その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知する暗号化手法通知手段を備えたことを特徴とする請求項１４記載のＡＶコンテンツ送信装置。
【請求項１６】前記暗号化鍵生成手段は、定期的または不定期に前記暗号化鍵を更新し、
前記暗号化手法選択手段が暗号化手法を前記第２の暗号化手法に切り替えるタイミングは、前記暗号化鍵生成手段が前記第１の暗号化手法において暗号化鍵を更新するタイミングであることを特徴とする請求項１４記載のＡＶコンテンツ送信装置。
【請求項１７】前記送信側認証・鍵交換手段は、前記認証要求をしたＡＶコンテンツ受信装置を記憶するとともに、そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなったと判断した場合、前記暗号化手法選択手段は、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とする請求項１４記載のＡＶコンテンツ送信装置。
【請求項１８】前記送信側認証・鍵交換手段は、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、
前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、
前記暗号化手法選択手段は、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とする請求項１４記載のＡＶコンテンツ送信装置。
【請求項１９】請求項１４から１８のいずれかに記載のＡＶコンテンツ送信装置との間で認証・鍵交換を行う受信側認証・鍵交換手段と、
前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツのその暗号化に利用された暗号化手法の情報を入力し、記憶する暗号化手法記憶手段と、
前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツを入力するとともに、前記ＡＶコンテンツ送信装置からの暗号化鍵またはその暗号化鍵の種を入力し、その後、前記暗号化手法記憶手段に記憶されている暗号化手法に基づき、かつ、前記暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する暗号解読手段とを備えたことを特徴とするＡＶコンテンツ受信装置。
【請求項２０】請求項１４から１８のいずれかに記載のＡＶコンテンツ送信装置から送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、
その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、
前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記情報に含まれていないものを送信するように要求する要求手段を備えたことを特徴とする請求項１９記載のＡＶコンテンツ受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、異なる暗号化手法で暗号化されたＡＶコンテンツの送信と、そのＡＶコンテンツの受信とに関するものである。
【０００２】
【従来の技術】近年、映画等のＡＶコンテンツをディジタル信号を用いて送信し、そのＡＶコンテンツを受信するといったことに関する技術が進歩してきている。
【０００３】そのようなＡＶコンテンツを送信する送信装置は、ＡＶコンテンツを送信する前に、内容を保護するという目的のために、ＡＶコンテンツの暗号化を行う。そして、受信装置は、暗号化されたＡＶコンテンツを受信し解読して、そのＡＶコンテンツの内容をモニタに表示する。
【０００４】さて、上述したように、送信装置はＡＶコンテンツを暗号化するが、その暗号化に用いる暗号化手

法には、複数の種類がある。例えば、受信装置がテレビ等の通常の家電機器であれば、そのような家電機器に対応させて、Ｍ６、Ｂlowfish等の'baseline cipher'と呼ばれる「基本暗号化手法」が用いられる。それに対して、例えば、受信装置がパソコン等の演算能力の高い機器であれば、ＤＥＳ等の暗号の強度がより高く、より複雑な「拡張暗号化手法」が用いられる。

【０００５】

【発明が解決しようとする課題】ところで、送信装置がパソコン等の演算能力の高い機器であって、ＩＥＥＥ１３９４バスを利用して、ＡＶコンテンツを送信し、そのＩＥＥＥ１３９４バスを介して、受信装置がＡＶコンテンツを受信する場合、上述したように、受信装置がパソコン等の演算能力の高い機器であれば、送信装置は「拡張暗号化手法」を使用してＡＶコンテンツを暗号化し送信しても、受信装置はそのＡＶコンテンツを解読することができるので、何等問題は起こらない。

【０００６】しかしながら、図６に示すように、例えば、パソコン２８という受信装置とともに、セットトップボックス（衛星放送受信機）２９のような通常の家電機器も、ＩＥＥＥ１３９４バスを介して送信装置２７に接続されている場合がある。その場合、送信装置２７が「拡張暗号化手法」を使用してＡＶコンテンツを暗号化して送信し、パソコン２８が受信し解読しているときに、その送信の途中から、セットトップボックス２９がそのＡＶコンテンツを受信し解読しようとしても、セットトップボックス２９は、「拡張暗号化手法」を使用することができないので、そのＡＶコンテンツを解読することができない。

【０００７】本発明は、上述したように、ＡＶコンテンツ送信装置が第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができないという課題を考慮して、ＡＶコンテンツ送信装置が第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法を提供することを目的とするものである。

【０００８】また、本発明は、第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信装置を提供することを目的とするものである。

【０００９】また、本発明は、上述したＡＶコンテンツ送信方法を用いたさい、第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、第１の暗号化手法を使用することができないＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、その別のＡＶコンテンツ受信装置が引き続きそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法およびＡＶコンテンツ受信方法を提供することを目的とするものである。

【００１０】さらに、本発明は、上述したＡＶコンテンツ送信装置が第１の暗号化手法を使用することができないＡＶコンテンツ受信装置にそのＡＶコンテンツを解読させる場合、そのＡＶコンテンツ受信装置とは別に、第１の暗号化手法で暗号化されていたＡＶコンテンツを引き続き解読するＡＶコンテンツ受信装置を提供することを目的とするものである。

【００１１】

【課題を解決するための手段】第１の本発明（請求項１に対応）は、ＡＶコンテンツ送信装置が伝送路を利用して第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、その認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法で前記ＡＶコンテンツを暗号化して送信することを特徴とするＡＶコンテンツ送信方法である。

【００１２】第２の本発明（請求項２に対応）は、第１の本発明のＡＶコンテンツ送信方法において、前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知することを特徴とするＡＶコンテンツ送信方法である。

【００１３】第３の本発明（請求項３に対応）は、第２の本発明のＡＶコンテンツ送信方法において、前記暗号化手法の切り替えを、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とするＡＶコンテンツ送信方法である。

【００１４】第４の本発明（請求項４に対応）は、第３の本発明のＡＶコンテンツ送信方法において、前記切り替えた後の前記第２の暗号化手法がどのような暗号化手法であるのかという情報を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とするＡＶコンテンツ送信方法である。

【００１５】第５の本発明（請求項５に対応）は、第３の本発明のＡＶコンテンツ送信方法において、前記切り替えた後の前記第２の暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を、所定のコマンドを用いて、または前記ＡＶコンテンツのなかに付加して通知することを特徴とするＡＶコンテンツ送信方法である。

【００１６】第６の本発明（請求項６に対応）は、第１の本発明のＡＶコンテンツ送信方法において、前記暗号

化手法の切り替えのタイミングを、前記認証要求がある前に使用していた前記第１の暗号化手法での暗号化鍵の更新のタイミングとすることを特徴とするＡＶコンテンツ送信方法である。

【００１７】第７の本発明（請求項７に対応）は、第２の本発明のＡＶコンテンツ送信方法において、少なくとも前記別のＡＶコンテンツ受信装置に、前記暗号化手法が前記第２の暗号化手法に切り替わることを通知するとともに、その暗号化手法の切り替えのタイミングの情報を送信することを特徴とするＡＶコンテンツ送信方法である。

【００１８】第８の本発明（請求項８に対応）は、第１の本発明のＡＶコンテンツ送信方法において、前記ＡＶコンテンツ送信装置が前記認証要求をしたＡＶコンテンツ受信装置を記憶し、そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなった場合、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とするＡＶコンテンツ送信方法である。

【００１９】第９の本発明（請求項９に対応）は、第１の本発明のＡＶコンテンツ送信方法において、前記ＡＶコンテンツ送信装置が、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とするＡＶコンテンツ送信方法である。

【００２０】第１０の本発明（請求項１０に対応）は、第１から第９のいずれかの本発明のＡＶコンテンツ送信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体である。

【００２１】第１１の本発明（請求項１１に対応）は、第１から第９のいずれかの本発明のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツを受信し、そのＡＶコンテンツが暗号化されたさいに使用された暗号化手法に基づくとともに、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読することを特徴とするＡＶコンテンツ受信方法である。

【００２２】第１２の本発明（請求項１２に対応）は、第１１の本発明のＡＶコンテンツ送信方法において、第１から第９のいずれかの本発明のＡＶコンテンツ送信方法によって送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記暗号化手法の切り替えに関する情報に含まれていないものを送信するように要求することを特徴とするＡＶコンテンツ受信方法である。

【００２３】第１３の本発明（請求項１３に対応）は、第１１または第１２の本発明のＡＶコンテンツ受信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体である。

【００２４】第１４の本発明（請求項１４に対応）は、送信しようとするＡＶコンテンツを暗号化するさいの暗号化手法を選択する暗号化手法選択手段と、その暗号化手法選択手段によって選択された暗号化手法に対応した、ＡＶコンテンツを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、ＡＶコンテンツを入力するとともに、前記暗号化鍵生成手段からの前記暗号化鍵を入力し、その暗号化鍵を利用して、前記ＡＶコンテンツを暗号化する暗号化手段と、ＡＶコンテンツ受信装置との間で認証・鍵交換を行う送信側認証・鍵交換手段とを備え、ＡＶコンテンツ送信装置が、前記暗号化手法選択手段によって選択された第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置から認証要求があると、前記送信側認証・鍵交換手段が、その認証要求をしたＡＶコンテンツ受信装置との間で認証を行い、前記暗号化手法選択手段が、暗号化手法を、前記認証要求をしたＡＶコンテンツ受信装置が使用することができる第２の暗号化手法に切り替えることを特徴とするＡＶコンテンツ送信装置である。

【００２５】第１５の本発明（請求項１５に対応）は、第１４の本発明のＡＶコンテンツ送信装置において、前記認証要求があったさい、既にそれまでの前記第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、前記認証要求をしたＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、その別のＡＶコンテンツ受信装置に、暗号化手法が前記第２の暗号化手法に切り替わることを通知する暗号化手法通知手段を備えたことを特徴とするＡＶコンテンツ送信装置である。

【００２６】第１６の本発明（請求項１６に対応）は、第１４の本発明のＡＶコンテンツ送信装置において、前記暗号化鍵生成手段が、定期的または不定期に前記暗号

化鍵を更新し、前記暗号化手法選択手段が暗号化手法を前記第２の暗号化手法に切り替えるタイミングが、前記暗号化鍵生成手段が前記第１の暗号化手法において暗号化鍵を更新するタイミングであることを特徴とするＡＶコンテンツ送信装置である。

【００２７】第１７の本発明（請求項１７に対応）は、第１４の本発明のＡＶコンテンツ送信装置において、前記送信側認証・鍵交換手段が、前記認証要求をしたＡＶコンテンツ受信装置を記憶するとともに、そのＡＶコンテンツ受信装置から、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドが来ているか否かを判断し、前記コマンドが来なくなったと判断した場合、前記暗号化手法選択手段が、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とするＡＶコンテンツ送信装置である。

【００２８】第１８の本発明（請求項１８に対応）は、第１４の本発明のＡＶコンテンツ送信装置において、前記送信側認証・鍵交換手段が、前記認証要求をしたＡＶコンテンツ受信装置と前記そのＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、前記ＡＶコンテンツを解読するための暗号化鍵またはその暗号化鍵の種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て前記第１の暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、前記暗号化手法選択手段が、前記暗号化手法を前記第２の暗号化手法から前記第１の暗号化手法に切り替えることを特徴とするＡＶコンテンツ送信装置である。

【００２９】第１９の本発明（請求項１９に対応）は、第１４から第１８のいずれかの本発明のＡＶコンテンツ送信装置との間で認証・鍵交換を行う受信側認証・鍵交換手段と、前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツのその暗号化に利用された暗号化手法の情報を入力し、記憶する暗号化手法記憶手段と、前記ＡＶコンテンツ送信装置からの暗号化されたＡＶコンテンツを入力するとともに、前記ＡＶコンテンツ送信装置からの暗号化鍵またはその暗号化鍵の種を入力し、その後、前記暗号化手法記憶手段に記憶されている暗号化手法に基づき、かつ、前記暗号化鍵またはその暗号化鍵の種を利用して、前記暗号化されたＡＶコンテンツを解読する暗号解読手段とを備えたことを特徴とするＡＶコンテンツ受信装置である。

【００３０】第２０の本発明（請求項２０に対応）は、第１９の本発明のＡＶコンテンツ受信装置において、第１４から第１８のいずれかの本発明のＡＶコンテンツ送信装置から送信されてくるＡＶコンテンツとともに、またはそのＡＶコンテンツのなかに、前記暗号化手法の切り替えに関する情報があって、その情報に、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種との一方または両方が含まれていない場合、前記ＡＶコンテンツ送信装置に対して、前記切り替え後の暗号化手法がどのような暗号化手法であるのかという情報と、その暗号化手法で使用する暗号化鍵またはその暗号化鍵の種とのうちの前記情報に含まれていないものを送信するように要求する要求手段を備えたことを特徴とするＡＶコンテンツ受信装置である。

【００３１】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【００３２】（実施の形態１）先ず、本発明の実施の形態１のＡＶコンテンツ通信システムの構成を述べる。

【００３３】図１に、本発明の実施の形態１のＡＶコンテンツ通信システムのブロック図を示す。図１に示すように、本発明の実施の形態１のＡＶコンテンツ通信システムは、ＡＶコンテンツ送信装置１と、第１のＡＶコンテンツ受信装置２と、第２のＡＶコンテンツ受信装置３と、ＩＥＥＥ１３９４バスから構成される。なお、図１には、アンテナ４と、モニタ５および６も表示する。

【００３４】さて、ＡＶコンテンツ送信装置１は、図１に示すように、受信手段７と、暗号化手段８と、Ｋｃｏ生成手段９と、暗号化手法選択手段１０と、ＡＫＥ手段１１と、暗号化手法変更通知手段１２と、Ｋｃｏ要求コマンド応答手段１３と、データ転送手段１４から構成される。

【００３５】受信手段７は、ＡＶコンテンツを、ＡＶコンテンツ送信装置１外部のアンテナ４を介して受信する手段である。

【００３６】暗号化手段８は、基本暗号化手法と拡張暗号化手法とを使用することができるものであって、受信手段７からのＡＶコンテンツを入力するとともに、Ｋｃｏ生成手段９からの暗号化鍵Ｋｃｏを入力し、暗号化手法選択手段１０によって選択された暗号化手法を使用し、暗号化鍵ＫｃｏでＡＶコンテンツを暗号化する手段である。なお、暗号化鍵Ｋｃｏで暗号化されたＡＶコンテンツを$Kco(AV)$とする。また、基本暗号化手法と拡張暗号化手法との相違は、暗号化の強度が異なるということであって、拡張暗号化手法の方が基本暗号化手法よりも暗号化の強度が強いものであるとする。さらにいうと、暗号化するさいに用いる暗号化鍵Ｋｃｏを構成するデジィタル信号の長さが異なり、例えば、基本暗号化手法は、４０ビットの暗号化鍵Ｋｃｏを用いてＡＶコンテンツを暗号化する手法であって、拡張暗号化手法は、５６ビットの暗号化鍵Ｋｃｏを用いてＡＶコンテンツを暗号化する手法であるものとする。

【００３７】Ｋｃｏ生成手段９は、暗号化手段８が受信手段７からのＡＶコンテンツを暗号化するさいに用いる暗号化鍵Ｋｃｏを生成する手段であって、その暗号化鍵

Ｋｃｏを２０秒毎に更新するものである。

【００３８】暗号化手法選択手段１０は、暗号化手段８がＡＶコンテンツを暗号化するさいに使用する暗号化手法を選択する手段である。

【００３９】ＡＫＥ手段１１は、第１のＡＶコンテンツ受信装置２との間で認証・鍵交換を行う手段であって、第１のＡＶコンテンツ受信装置２との間で認証が成功した場合、その第１のＡＶコンテンツ受信装置２に対して、交換鍵Ｋｅｘ（ＥxchangeKey）を発行する手段である。また同様に、ＡＫＥ手段１１は、第２のＡＶコンテンツ受信装置３との間で認証・鍵交換を行う手段でもある。

【００４０】暗号化手法変更通知手段１２は、それまでに選択していた暗号化手法からそれとは別の暗号化手法に暗号化手法の選択を変更する場合、その変更を通知する手段である。

【００４１】Ｋｃｏ要求コマンド応答手段１３は、第１のＡＶコンテンツ受信装置２および／または第２のＡＶコンテンツ受信装置３からの、２０秒毎に更新される最新の暗号化鍵Ｋｃｏの種を送信するように要求されたコマンドを入力し、そのコマンドにしたがって暗号化鍵Ｋｃｏの種を送信する手段である。

【００４２】データ転送手段１４は、ＡＶコンテンツ送信装置１の各構成手段と第１のＡＶコンテンツ受信装置２および／または第２のＡＶコンテンツ受信装置３との間でのデータ通信の仲介を行う手段である。

【００４３】次に、第１のＡＶコンテンツ受信装置２は、図１に示すように、データ転送手段１５と、ＡＫＥ手段１６と、暗号化手法通知検出手段１７と、Ｋｃｏ要求コマンド発行手段１８と、Ｋｃｏ記憶手段１９と、暗号化手法記憶手段２０と、暗号解読手段２１から構成される。

【００４４】データ転送手段１５は、第１のＡＶコンテンツ受信装置２の各構成手段とＡＶコンテンツ送信装置１との間でのデータ通信の仲介を行う手段である。

【００４５】ＡＫＥ手段１６は、ＡＶコンテンツ送信装置１との間で認証・鍵交換を行う手段であって、ＡＶコンテンツ送信装置１との間で認証が成功した場合、そのＡＶコンテンツ送信装置１から交換鍵Ｋｅｘを入力する手段である。

【００４６】暗号化手法通知検出手段１７は、ＡＶコンテンツ送信装置１からのＡＶコンテンツの暗号化に使用された暗号化手法がどのような暗号化手法であるのかを検出する手段である。

【００４７】Ｋｃｏ要求コマンド発行手段１８は、暗号化手法通知検出手段１７によって検出された暗号化手法にしたがって、その暗号化手法に対応する暗号化鍵Ｋｃｏの種を送信するようにＡＶコンテンツ送信装置１に対して要求するコマンドを発行する手段である。また、Ｋｃｏ要求コマンド発行手段１８は、その要求コマンドに対応する、ＡＶコンテンツ送信装置１からの暗号化鍵Ｋｃｏの種を入力する手段でもある。

【００４８】Ｋｃｏ記憶手段１９は、あらかじめ、ＡＶコンテンツ送信装置１からの暗号化されたＡＶコンテンツを解読するさいに必要となる所定の関数が設定されており、ＡＫＥ手段１６からの交換鍵Ｋｅｘを入力するとともに、Ｋｃｏ要求コマンド発行手段１８からの暗号化鍵Ｋｃｏの種を入力し、交換鍵Ｋｅｘと暗号化鍵Ｋｃｏとをあらかじめ設定されている関数に代入して暗号化鍵Ｋｃｏを生成し記憶する手段である。なお、その関数については後に述べることにする。

【００４９】暗号化手法記憶手段２０は、暗号化手法通知検出手段１７によって検出された暗号化手法を記憶する手段である。

【００５０】暗号解読手段２１は、ＡＶコンテンツ送信装置１からの暗号化されたＡＶコンテンツを入力するとともに、Ｋｃｏ記憶手段１９からの暗号化鍵Ｋｃｏと、暗号化手法記憶手段２０からの暗号化手法とを入力し、その暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏで解読する手段である。なお、暗号解読手段２１は、基本暗号化手法と拡張暗号化手法のいずれもを使用することができるものであるとする。

【００５１】次に、第２のＡＶコンテンツ受信装置３は、図１に示すように、データ転送手段２２と、ＡＫＥ手段２３と、Ｋｃｏ要求コマンド発行手段２４と、Ｋｃｏ記憶手段２５と、暗号解読手段２６から構成される。

【００５２】データ転送手段２２は、第２のＡＶコンテンツ受信装置３の各構成手段とＡＶコンテンツ送信装置１との間でのデータ通信の仲介を行う手段である。

【００５３】ＡＫＥ手段２３は、ＡＶコンテンツ送信装置１との間で認証・鍵交換を行う手段であって、ＡＶコンテンツ送信装置１との間で認証が成功した場合、そのＡＶコンテンツ送信装置１から交換鍵Ｋｅｘを入力する手段である。

【００５４】Ｋｃｏ要求コマンド発行手段２４は、基本暗号化手法に対応する暗号化鍵Ｋｃｏの種を送信するようにＡＶコンテンツ送信装置１に対して要求するコマンドを発行する手段である。また、Ｋｃｏ要求コマンド発行手段２４は、その要求コマンドに対応する、ＡＶコンテンツ送信装置１からの最新の暗号化鍵Ｋｃｏの種を入力する手段でもある。

【００５５】Ｋｃｏ記憶手段２６は、あらかじめ、ＡＶコンテンツ送信装置１からの暗号化されたＡＶコンテンツを解読するさいに必要となる所定の関数が設定されており、ＡＫＥ手段２３からの交換鍵Ｋｅｘを入力するとともに、Ｋｃｏ要求コマンド発行手段２４からの暗号化鍵Ｋｃｏの種を入力し、交換鍵Ｋｅｘと暗号化鍵Ｋｃｏとをあらかじめ設定されている関数に代入して暗号化鍵Ｋｃｏを生成し記憶する手段である。

【００５６】暗号解読手段２６は、ＡＶコンテンツ送信

装置１からの暗号化されたＡＶコンテンツを入力するとともに、Ｋｃｏ記憶手段２５からの暗号化鍵Ｋｃｏを入力し、基本暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏで解読する手段である。なお、暗号解読手段２６は、基本暗号化手法のみを使用することができるものであるとする。いいかえると、暗号解読手段２６は、拡張暗号化手法を使用することができないものである。

【００５７】次に、ＩＥＥＥ１３９４バスは、ＡＶコンテンツ送信装置１、第１のＡＶコンテンツ受信装置２および第２のＡＶコンテンツ受信装置３それぞれの間で通信されるデータの伝送路である。

【００５８】また、アンテナ４は、ＡＶコンテンツ送信装置１外部に設置され、ＡＶコンテンツを受信する手段である。モニタ５は、第１のＡＶコンテンツ受信装置２からのＡＶコンテンツを表示する手段であり、同様に、モニタ６は、第２のＡＶコンテンツ受信装置３からのＡＶコンテンツを表示する手段である。

【００５９】次に、本発明の実施の形態１のＡＶコンテンツ通信システムの動作を述べる。

【００６０】図１のＡＶコンテンツ通信システムの動作を詳しく述べる前に、以下の説明の便宜上、次に示す状況を想定し、その状況下でのＡＶコンテンツ通信システムの動作を述べることにする。

【００６１】その状況とは、先ず、ＡＶコンテンツ送信装置１がアンテナ４からのＡＶコンテンツを拡張暗号化手法を用いて暗号化してＩＥＥＥ１３９４バスに出力しており、そのＡＶコンテンツの出力の途中から、第１のＡＶコンテンツ受信装置２がそのＡＶコンテンツを受信して解読し、さらにその後、拡張暗号化手法を使用することができない第２のＡＶコンテンツ受信装置３がそのＡＶコンテンツを受信して解読しようとする状況である。

【００６２】さて、はじめに、ＡＶコンテンツ送信装置１がアンテナ４からのＡＶコンテンツを拡張暗号化手法を用いて暗号化しＩＥＥＥ１３９４バスに出力するまでのＡＶコンテンツ送信装置１の動作を述べる。なお、ＡＶコンテンツ送信装置１は、上述したように、拡張暗号化手法を使用することもできるし、基本暗号化手法を使用することもできるが、出力するＡＶコンテンツの内容をより強く保護するという目的のために、基本暗号化手法を使用して暗号化したＡＶコンテンツを出力するようにを要求されることがなければ、暗号化強度のより強い拡張暗号化手法を使用してＡＶコンテンツを暗号化するものとする。

【００６３】先ず、暗号化手法選択手段１０は、拡張暗号化手法を選択し、受信手段７は、ＡＶコンテンツ送信装置１外部のアンテナ４を介してＡＶコンテンツを受信し、暗号化手段８は、受信手段７からのＡＶコンテンツを入力するとともに、Ｋｃｏ生成手段９からの暗号化鍵Ｋｃｏ１を入力し、その後、拡張暗号化手法に基づいて、暗号化鍵Ｋｃｏ１でＡＶコンテンツを暗号化する。なお、Ｋｃｏ生成手段９からの暗号化鍵を、拡張暗号化手法に対応する暗号化鍵であることを示すために、「Ｋｃｏ１」というように記述した。また、以下では、その拡張暗号化手法とは別の基本暗号化手法に対応する暗号化鍵を「Ｋｃｏ２」というように記述する。ところで、暗号化は、例えばＡＶコンテンツの一部のヘッダについては行われないものとする。つまり、ＡＶコンテンツが受信されたさいに、暗号化鍵Ｋｃｏ１がなくてもそのＡＶコンテンツのヘッダ情報は解読されるが、そのＡＶコンテンツの内容は暗号化鍵Ｋｃｏ１がなくては解読されないように暗号化が行われるものとする。また、暗号化手段８が利用するＫｃｏ生成手段９からの暗号化鍵Ｋｃｏ１は、上述したように２０秒毎に更新されるものとする。そして、Ｋｃｏ生成手段９は、暗号化鍵Ｋｃｏ１がどのタイミングで更新するのかという情報として、ｏｄｄまたはｅｖｅｎを出力する。そのｏｄｄまたはｅｖｅｎは、互いに相手方から切り替わったときに、その切り替わりの前後でＡＶコンテンツの暗号化に使用された暗号化鍵Ｋｃｏ１が２０秒毎の更新により切り替わっていることを示すためのものであるとする。その後、データ転送手段１４は、暗号化手段８からの暗号化鍵Ｋｃｏ１で暗号化されたＡＶコンテンツ、つまりＫｃｏ（ＡＶコンテンツ）を入力するとともに、Ｋｃｏ生成手段９からのｏｄｄまたはｅｖｅｎを入力し、図２（ａ）に示すように、Ｋｃｏ（ＡＶコンテンツ）のヘッダのなかにｏｄｄまたはｅｖｅｎを付加してＩＥＥＥ１３９４バスに出力する。なお、図２（ａ）は、ＡＶコンテンツ送信装置１から送信されるＡＶコンテンツの構成図である。図２（ｂ）については後に説明する。

【００６４】次に、上述したようにしてＡＶコンテンツ送信装置１がＡＶコンテンツを暗号化してＩＥＥＥ１３９４バスに出力しているときに、その途中から、第１のＡＶコンテンツ受信装置２がそのＡＶコンテンツを解読するところまでのＡＶコンテンツ送信装置１と第１のＡＶコンテンツ受信装置２の動作を述べる。

【００６５】このとき、第１のＡＶコンテンツ受信装置２のＡＫＥ手段１６は、ＡＶコンテンツ送信装置１のＡＫＥ手段１１に対して、認証要求を行い、ＡＫＥ手段１６およびＡＫＥ手段１１は、互いに相手方の装置の認証を行う。その認証が成功すると、ＡＫＥ手段１１は、ＡＫＥ手段１６に交換鍵Ｋｅｘを出力する。その交換鍵Ｋｅｘは、暗号化されたＡＶコンテンツを解読するさいに必要となる鍵である。それとともに、ＡＫＥ手段１１は、第１のＡＶコンテンツ受信装置２が拡張暗号化手法を使用することができるものであることを判断し、暗号化手法の変更を行わない。なお、ＡＫＥ手段１６およびＡＫＥ手段１１が行う認証が失敗した場合、ＡＫＥ手段１１は、ＡＫＥ手段１６に交換鍵Ｋｅｘを出力すること

はない。ここでは、以下の説明の便宜上、ＡＫＥ手段１６およびＡＫＥ手段１１が行う認証は成功するものとする。そして、第１のＡＶコンテンツ受信装置２のＡＫＥ手段１６は、データ転送手段１５を介して、ＡＫＥ手段１１からの交換鍵Ｋｅｘを入力し、Ｋｃｏ記憶手段１９に出力する。また、暗号化手法通知検出手段１７は、ＡＶコンテンツ送信装置１からのＡＶコンテンツが拡張暗号化手法で暗号化されたものであることを検出し、その旨の情報、つまり拡張暗号化手法を暗号化手法記憶手段２０に出力し記憶させる。さらに、Ｋｃｏ要求コマンド発行手段１８は、拡張暗号化手法に対応する最新の暗号化鍵Ｋｃｏ１の種を送信するように、ＡＶコンテンツ送信装置１のＫｃｏ要求コマンド応答手段１３に対してコマンドを発行し、そのコマンドに対応するＫｃｏ要求コマンド応答手段１３からの最新の暗号化鍵Ｋｃｏ１の種を入力して、その種をＫｃｏ記憶手段１９に出力する。なお、上述したように、ＡＶコンテンツ送信装置１からの暗号化鍵Ｋｃｏ１が２０秒毎に更新されるので、Ｋｃｏ要求コマンド発行手段１８は、Ｋｃｏ要求コマンド応答手段１３に対するコマンドを２０秒毎に発行するものとする。その後、Ｋｃｏ記憶手段１９は、後述する（数１）に示すように、あらかじめ設定されている関数に、ＡＫＥ手段１６からの交換鍵Ｋｅｘと、Ｋｃｏ要求コマンド発行手段１８からの暗号化鍵Ｋｃｏ１の種とを代入し、暗号化鍵Ｋｃｏ１を生成し記憶する。ただし、（数１）のｓｅｅｄのところに、暗号化鍵Ｋｃｏ１の種を代入する。

【００６６】

【数１】Ｋｃｏ＝ｆ（ｓｅｅｄ，Ｋｅｘ）

そして、ＡＶコンテンツ送信装置１からのＫｃｏ（ＡＶコンテンツ）のヘッダのなかのｏｄｄまたはｅｖｅｎを検出し、さらに、ｏｄｄとｅｖｅｎとの切り替わりを判断して、ＡＶコンテンツ送信装置１からのＫｃｏ（ＡＶコンテンツ）がどの暗号化鍵Ｋｃｏ１で暗号化されたのかを特定する。なお、上述したように、ｏｄｄとｅｖｅｎとの切り替わりは、その切り替わりの前後でＡＶコンテンツの暗号化に使用された暗号化鍵Ｋｃｏ１が切り替わっていることを示す。また、ＡＶコンテンツ送信装置１のＫｃｏ要求コマンド応答手段１３は、Ｋｃｏ要求コマンド発行手段１８からの、暗号化鍵Ｋｃｏ１の種の送信要求のコマンドを入力すると、そのコマンドにしたがって、暗号化鍵Ｋｃｏ１の種をデータ転送手段１４に出力する。そして、データ転送手段１４は、図２に示すように、Ｋｃｏ（ＡＶコンテンツ）に使用した暗号化鍵Ｋｃｏ１の種を、Ｋｃｏ（ＡＶコンテンツ）とは別の非同期信号を使用してコマンドでＩＥＥＥ１３９４バスに出力する。なお、図２（ｂ）は、ＡＶコンテンツ送信装置１から送信されるコマンドの構成図である。

【００６７】最後に、暗号解読手段２１は、ＡＶコンテンツ送信装置１からの暗号化されたＡＶコンテンツをデータ転送手段１５を介して入力するとともに、Ｋｃｏ記憶手段１９からの暗号化鍵Ｋｃｏ１と、暗号化手法記憶手段２０からの拡張暗号化手法とを入力し、その拡張暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏ１で解読し、モニタ５に出力する。そして、モニタ５は、暗号解読手段２１からのＡＶコンテンツの内容を表示する。

【００６８】次に、上述したようにして、ＡＶコンテンツ送信装置１が拡張暗号化手法を使用してＡＶコンテンツを暗号化して出力し、第１のＡＶコンテンツ受信装置２がそのＡＶコンテンツを解読しているときに、拡張暗号化手法を使用することができない第２のＡＶコンテンツ受信装置３がそのＡＶコンテンツを解読するさいのＡＶコンテンツ送信装置１、第１のＡＶコンテンツ受信装置２および第２のＡＶコンテンツ受信装置３の動作を述べる。なお、そのさいのＡＶコンテンツ送信装置１の動作については図３のフローチャートをも用いて説明する。

【００６９】さて、第２のＡＶコンテンツ受信装置３のＡＫＥ手段２３は、ＡＶコンテンツ送信装置１のＡＫＥ手段１１に対して、認証要求を行い、ＡＫＥ手段２３およびＡＫＥ手段１１は、互いに相手方の装置の認証を行う（図３のステップ１）。そのさい、ＡＫＥ手段２３は、ＡＶコンテンツ送信装置１が出力するＡＶコンテンツの暗号化手法を、基本暗号化手法にするように要求する。なぜなら、第２のＡＶコンテンツ受信装置３は、拡張暗号化手法を使用することができず、基本暗号化手法しか使用することができないからである。そして、互いの認証が成功すると、ＡＫＥ手段１１は、その要求を受け入れ（図３のステップ２）、暗号化手法選択手段１０および暗号化手法変更通知手段１２に、暗号化手法を基本暗号化手法にするように制御するための情報を出力する（図３のステップ３）。その後、ＡＫＥ手段１１は、ＡＫＥ手段２３に交換鍵Ｋｅｘを出力し、ＡＫＥ手段１１とＡＫＥ手段２３との間の認証・鍵交換は完了する（図３のステップ４）。なお、交換鍵Ｋｅｘは、暗号化されたＡＶコンテンツを解読するさいに必要となる鍵である。また、ＡＫＥ手段２３およびＡＫＥ手段１１が行う認証が失敗した場合、ＡＫＥ手段１１は、ＡＫＥ手段２３に交換鍵Ｋｅｘを出力することもないし、暗号化手法を基本暗号化手法にするようにとの要求を受け入れることもない。ただしここでは、以下の説明の便宜上、ＡＫＥ手段２３およびＡＫＥ手段１１が行う認証は成功するものとする。

【００７０】そして、ＡＶコンテンツ送信装置１では、暗号化手法選択手段１０が、ＡＫＥ手段１１からの、暗号化手法を基本暗号化手法にするための情報、つまり暗号化手法を変更させるための情報にしたがって、基本暗号化手法を選択し、その旨の情報を、暗号化手段８とＫｃｏ生成手段９とに出力する。なお、暗号化手法選択手

段１０は、ＡＫＥ手段１１とＡＫＥ手段２３との間の認証・鍵交換が完了するまでに、いいかえると、ＡＫＥ手段２３が交換鍵Ｋｅｘを入力するまでに、基本暗号化手法を選択する。その後、Ｋｃｏ生成手段９は、その暗号化手法の基本暗号化手法への変更の情報を入力した後であって、かつ、拡張暗号化手法にしたがって生成していた暗号化鍵Ｋｃｏ１の次の更新タイミングから、基本暗号化手法にしたがった暗号化鍵Ｋｃｏ２を生成し、２０秒毎に更新してゆく。また、暗号化手法変更通知手段１２は、ＡＶコンテンツの暗号化手法を拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを、第１のＡＶコンテンツ受信装置２の暗号化手法通知検出手段１７に出力するとともに、その暗号化手法の切り替えのタイミングの情報のコマンドを暗号化手法通知検出手段１７に出力する。

【００７１】その後、ＡＶコンテンツ送信装置１の暗号化手段８は、受信手段７からのＡＶコンテンツを入力するとともに、Ｋｃｏ生成手段９からの暗号化鍵Ｋｃｏ２を入力し、基本暗号化手法に基づいて、暗号化鍵Ｋｃｏ２でＡＶコンテンツを暗号化する。さらに、Ｋｃｏ生成手段９は、暗号化鍵Ｋｃｏ２がどのタイミングで切り替わるのかという情報としてｏｄｄまたはｅｖｅｎを出力する。そして、データ転送手段１４は、暗号化手段８からの暗号化鍵Ｋｃｏ２で暗号化されたＡＶコンテンツ、つまりＫｃｏ（ＡＶコンテンツ）を入力するとともに、Ｋｃｏ生成手段９からのｏｄｄまたはｅｖｅｎを入力し、Ｋｃｏ（ＡＶコンテンツ）のヘッダのなかにｏｄｄまたはｅｖｅｎを付加してＩＥＥＥ１３９４バスに出力する。

【００７２】このようにＡＶコンテンツ送信装置１からのＡＶコンテンツの暗号化手法が基本暗号化手法に切り替わると、第２のＡＶコンテンツ受信装置３は、そのＡＶコンテンツを解読することができるようになる。そこで次に、このときの第２のＡＶコンテンツ受信装置３がＡＶコンテンツを解読するさいの動作を述べる。

【００７３】先ず、ＡＫＥ手段２３は、ＡＶコンテンツ送信装置１のＡＫＥ手段１１からの交換鍵Ｋｅｘを、データ転送手段２２を介して入力し、Ｋｃｏ記憶手段２５に出力する。また、Ｋｃｏ要求コマンド発行手段２４は、基本暗号化手法に対応する暗号化鍵Ｋｃｏ２の種を送信するように、ＡＶコンテンツ送信装置１のＫｃｏ要求コマンド応答手段１３に対してコマンドを発行し、そのコマンドに対応する、Ｋｃｏ要求コマンド応答手段１３からの暗号化鍵Ｋｃｏ２の種を入力して、その種をＫｃｏ記憶手段２５に出力する。その後、Ｋｃｏ記憶手段２５は、（数１）を用いて上述したようにして、あらかじめ設定されている関数に、ＡＫＥ手段２３からの交換鍵Ｋｅｘと、Ｋｃｏ要求コマンド発行手段２４からの暗号化鍵Ｋｃｏ２の種とを代入し、暗号化鍵Ｋｃｏ２を生成し記憶する。そして、ＡＶコンテンツ送信装置１からのＫｃｏ（ＡＶコンテンツ）のヘッダのなかのｏｄｄまたはｅｖｅｎを検出し、さらに、ｏｄｄとｅｖｅｎとの切り替わりを判断して、ＡＶコンテンツ送信装置１からのＫｃｏ（ＡＶコンテンツ）がどの暗号化鍵Ｋｃｏ２で暗号化されたのかを特定する。

【００７４】最後に、暗号解読手段２６は、ＡＶコンテンツ送信装置１からの暗号化されたＡＶコンテンツをデータ転送手段２２を介して入力するとともに、Ｋｃｏ記憶手段２５からの暗号化鍵Ｋｃｏ２を入力し、基本暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏ２で解読し、モニタ６に出力する。そして、モニタ６は、暗号解読手段２６からのＡＶコンテンツの内容を表示する。

【００７５】このように、ＡＶコンテンツ送信装置１がＡＶコンテンツの暗号化手法を基本暗号化手法に変更してＡＶコンテンツを暗号化し出力すると、第２のＡＶコンテンツ受信装置３は、そのＡＶコンテンツを解読することができるようになるが、それまで拡張暗号化手法によって暗号化されたＡＶコンテンツを受信し解読していた第１のＡＶコンテンツ受信装置２は、そのままでは、そのＡＶコンテンツを解読することができなくなる。そこで次に、ＡＶコンテンツ送信装置１がＡＶコンテンツの暗号化手法を基本暗号化手法に変更した場合、第１のＡＶコンテンツ受信装置２がそのＡＶコンテンツを解読するさいの、第１のＡＶコンテンツ受信装置２の動作を述べる。なお、そのさいの第１のＡＶコンテンツ受信装置２の動作については図４のフローチャートをも用いて説明する。

【００７６】さてそのとき、上述したように、第１のＡＶコンテンツ受信装置２の暗号化手法通知検出手段１７は、ＡＶコンテンツ送信装置１の暗号化手法変更通知手段１２からの、ＡＶコンテンツの暗号化手法が拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを入力するとともに、その暗号化手法の切り替えのタイミングの情報のコマンドも入力する（図４のステップ１）。そして、暗号化手法通知検出手段１７は、それら２つの情報を、Ｋｃｏ要求コマンド発行手段１８と暗号化手法記憶手段２０とに出力する。その後、Ｋｃｏ要求コマンド発行手段１８は、基本暗号化手法に対応する暗号化鍵Ｋｃｏ２の種を送信するように、ＡＶコンテンツ送信装置１のＫｃｏ要求コマンド応答手段１３に対してコマンドを発行し（図４のステップ２）、そのコマンドに対応する、Ｋｃｏ要求コマンド応答手段１３からの暗号化鍵Ｋｃｏ２の種を入力して、その種をＫｃｏ記憶手段１９に出力する。その後、Ｋｃｏ記憶手段１９は、あらかじめ設定されている関数に、ＡＫＥ手段１６からの交換鍵Ｋｅｘと、Ｋｃｏ要求コマンド発行手段１８からの暗号化鍵Ｋｃｏ２の種とを代入し、暗号化鍵Ｋｃｏ２を生成し記憶する（図４のステップ３）。

【００７７】最後に、暗号解読手段２１は、ＡＶコンテ

ンツ送信装置１からの暗号化されたＡＶコンテンツをデータ転送手段１５を介して入力するとともに、Ｋｃｏ記憶手段１９からの暗号化鍵Ｋｃｏ２と、暗号化手法記憶手段２０からの基本暗号化手法とを入力する。そして、暗号解読手段２１は、基本暗号化手法を使用することができるので、その基本暗号化手法に基づいて、暗号化されたＡＶコンテンツを暗号化鍵Ｋｃｏ２で解読し、モニタ５に出力する（図４のステップ４）。そして、モニタ５は、暗号解読手段２１からのＡＶコンテンツの内容を表示する。

【００７８】このように、ＡＶコンテンツ送信装置１がＡＶコンテンツの暗号化手法を基本暗号化手法に変更した場合であっても、第１のＡＶコンテンツ受信装置２は、暗号化手法が基本暗号化手法に切り替わったという情報と、その切り替えのタイミングの情報とを入力することによって、基本暗号化手法によって暗号化されたＡＶコンテンツを解読することができるようになる。

【００７９】ところで、ＡＶコンテンツ送信装置１がＡＶコンテンツの暗号化手法を基本暗号化手法に変更してＡＶコンテンツを送信しているとき、第２のＡＶコンテンツ受信装置３がそのＡＶコンテンツを解読することを中止することがある。以下に、そのような第２のＡＶコンテンツ受信装置３がＡＶコンテンツを解読することを中止する場合のＡＶコンテンツ送信装置１および第１のＡＶコンテンツ受信装置２の動作を述べる。

【００８０】さて、第２のＡＶコンテンツ受信装置３がＡＶコンテンツを解読することを中止する場合、第２のＡＶコンテンツ受信装置３のＫｃｏ要求コマンド発行手段２４は、暗号化鍵Ｋｃｏ２の種を送信するように、ＡＶコンテンツ送信装置１のＫｃｏ要求コマンド応答手段１３に対してコマンドを発行しなくなる。つまり、Ｋｃｏ要求コマンド応答手段１３にとっては、Ｋｃｏ要求コマンド発行手段２４からのコマンドを受信しなくなるということである。このように、Ｋｃｏ要求コマンド応答手段１３は、Ｋｃｏ要求コマンド発行手段２４からのコマンドを受信しなくなると、第２のＡＶコンテンツ受信装置３がＡＶコンテンツを解読することを中止したものと判断する。そして、Ｋｃｏ要求コマンド応答手段１３は、第２のＡＶコンテンツ受信装置３がＡＶコンテンツを解読することを中止したことを、暗号化手法変更通知手段１２に通知する。

【００８１】その後、暗号化手法変更通知手段１２は、Ｋｃｏ要求コマンド応答手段１３からの、第２のＡＶコンテンツ受信装置３がＡＶコンテンツを解読することを中止したとする情報を入力し、その情報に基づいて、暗号化手法選択手段１０に対して、選択する暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えさせるとともに、第１のＡＶコンテンツ受信装置２の暗号化手法通知検出手段１７に対して、暗号化手法が基本暗号化手法から拡張暗号化手法に切り替わるという情報を、その切り替えのタイミングの情報とともに出力する。このように、暗号化手法を拡張暗号化手法に切り替えるのは、上述したように拡張暗号化手法の方が基本暗号化手法よりも暗号化の強度が強く、不正な装置にＡＶコンテンツの内容を解読させないようにする防御をより強くするためである。なお、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるさい、あらかじめＡＫＥ手段１１に、第２のＡＶコンテンツ受信装置３が基本暗号化手法しか使用することができないということを記憶させておき、その後、暗号化手法変更通知手段１２に、第２のＡＶコンテンツ受信装置３がＡＶコンテンツを解読することを中止した場合、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるように判断させればよい。

【００８２】そして、暗号化手法選択手段１０は、暗号化手法の選択を基本暗号化手法から拡張暗号化手法に再度切り替える。このように暗号化手法が拡張暗号化手法に切り替えられた後のＡＶコンテンツ送信装置１の各構成手段は、上述した基本暗号化手法に切り替えられる前の拡張暗号化手法に基づいてＡＶコンテンツを暗号化し出力していたときと同じ動作を行う。

【００８３】他方、第１のＡＶコンテンツ受信装置２では、暗号化手法通知検出手段１７が、ＡＶコンテンツ送信装置１の暗号化手法変更通知手段１２からの、暗号化手法が基本暗号化手法から拡張暗号化手法に切り替わるという情報と、その切り替えのタイミングの情報とを入力する。そして、その情報にしたがって、暗号解読するさいの各構成手段が動作を切り替える。その切り替わりのタイミングは、暗号化手法が拡張暗号化手法から基本暗号化手法に切り替わったタイミングと同様に行われ、またその切り替え後の第１のＡＶコンテンツ受信装置２の各構成手段は、上述した基本暗号化手法に切り替えられる前の拡張暗号化手法に基づいて暗号化されたＡＶコンテンツを解読するさいの動作と同じように動作する。

【００８４】このように、ＡＶコンテンツ送信装置１がＡＶコンテンツの暗号化手法を基本暗号化手法を使用して暗号化しＡＶコンテンツを送信しているとき、第２のＡＶコンテンツ受信装置３がそのＡＶコンテンツを解読することを中止した場合、ＡＶコンテンツ送信装置１は、暗号化強度のより強い拡張暗号化手法で暗号化したＡＶコンテンツを送信するように変更する。このように暗号化手法が基本暗号化手法から拡張暗号化手法に変更された場合であっても、第１のＡＶコンテンツ受信装置２は、それに対応してそのＡＶコンテンツを解読することができる。

【００８５】なお、上述した実施の形態１では、ＡＶコンテンツ送信装置１の暗号化手法変更通知手段１２は、ＡＶコンテンツの暗号化手法が拡張暗号化手法から基本暗号化手法に変更するという旨の情報のコマンドを第１のＡＶコンテンツ受信装置２の暗号化手法通知検出手段１７に出力するとした。しかしながら、暗号化手法変更

通知手段１２は、ＡＶコンテンツの暗号化手法が拡張暗号化手法から他の暗号化手法に変更するという旨の情報を暗号化手法通知検出手段１７に出力するとしてもよい。ただしこの場合、暗号化手法通知検出手段１７は、変更後の暗号化手法がどのような暗号化手法であるのかを通知するように、ＡＶコンテンツ送信装置１に要求しなければならない。同様に、暗号化手法変更通知手段１２は、暗号化手法の拡張暗号化手法から基本暗号化手法への切り替えのタイミングの情報をコマンドで暗号化手法通知検出手段１７に出力するとしたが、暗号化手法変更通知手段１２は、そのような暗号化手法の切り替えのタイミングの情報を暗号化手法通知検出手段１７に出力しないとしてもよい。ただしこの場合も、暗号化手法通知検出手段１７は、暗号化手法の切り替えのタイミングの情報を通知するように、ＡＶコンテンツ送信装置１に要求しなければならない。また、暗号化手法変更通知手段１２が出力する暗号化手法の切り替えの情報や切り替えのタイミングの情報は、コマンドではなく、ＡＶコンテンツのなかに付加されたものであってもよい。

【００８６】また、上述した実施の形態１では、ＡＶコンテンツ送信装置１は、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるさい、暗号化手法のみがどのような暗号化手法に切り替わるのかという情報を出力し、その後、第１のＡＶコンテンツ受信装置２から、その変更後の暗号化手法に対応する暗号化鍵Ｋｃｏの種を送信するように要求された場合、その要求にしたがって、暗号化鍵Ｋｃｏの種を送信するとした。しかしながら、ＡＶコンテンツ送信装置１は、暗号化手法を切り替えるさい、切り替わった後の暗号化手法の情報とともに、その変更後の暗号化手法に対応する暗号化鍵Ｋｃｏの種を出力するとしてもよい。また、ＡＶコンテンツ送信装置１は、暗号化鍵Ｋｃｏの種を出力するとしたが、暗号化鍵Ｋｃｏそのもの、または交換鍵Ｋｅｘで暗号化した暗号化鍵Ｋｃｏを出力してもよい。その場合、受信側では、種ではなく、暗号化鍵Ｋｃｏそのもの、または交換鍵Ｋｅｘで暗号化された暗号化鍵Ｋｃｏが使用されることになる。また、暗号化鍵Ｋｃｏの種はコマンドを利用して送信されるとしたが、暗号化鍵Ｋｃｏやその種は、コマンドで送信されても、ＡＶコンテンツのなかに付加されて送信されてもよい。

【００８７】また、上述した実施の形態１では、ＡＶコンテンツ送信装置１のＫｃｏ生成手段９は、２０秒毎に暗号化鍵Ｋｃｏを更新するとしたが、Ｋｃｏ生成手段９が暗号化鍵Ｋｃｏを更新する間隔は、２０秒毎という間隔に限定されるものではない。暗号化鍵Ｋｃｏは、定期的に更新されてもよいし、不定期に更新されてもよい。

【００８８】また、上述した実施の形態１では、ＡＶコンテンツ送信装置１が第２のＡＶコンテンツ受信装置３を記憶し、その第２のＡＶコンテンツ受信装置３から、ＡＶコンテンツを解読するための暗号化鍵Ｋｃｏ２の種を要求するコマンドが来ているか否かを判断し、そのコマンドが来なくなった場合、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、ＡＶコンテンツ送信装置１が、第１のＡＶコンテンツ受信装置２と第２のＡＶコンテンツ受信装置３とについて、それぞれ使用することができる暗号化手法がどのような暗号化手法であるのかということを調べておき、ＡＶコンテンツを解読するための暗号化鍵Ｋｃｏの種を要求するコマンドを送信してくるＡＶコンテンツ受信装置が、全て拡張暗号化手法を使用することができるＡＶコンテンツ受信装置である場合、暗号化手法を基本暗号化手法から拡張暗号化手法に切り替えるとしてもよい。

【００８９】また、上述した実施の形態１では、ＡＶコンテンツ送信装置１が暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるさい、まず、ＡＶコンテンツ送信装置１は、第２のＡＶコンテンツ受信装置３との間で互いに認証を行い、その認証が成功すると、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、図５に示すように、ＡＶコンテンツ送信装置１は、第２のＡＶコンテンツ受信装置３からの認証要求を受信した後（図５のステップ１）、互いの認証が成功するか否かにかかわらず、暗号化手法を拡張暗号化手法から基本暗号化手法へ変更し（図５のステップ２）、その変更の後、認証が成功すると（図５のステップ３）、暗号化手法を基本暗号化手法に決定するとしてもよい（図５のステップ５）。なお、図５のステップ３で認証が失敗すると、暗号化手法を基本暗号化手法から拡張暗号化手法に再変更して暗号化手法を決定するとしてもよい（図５のステップ４）。

【００９０】また、上述した実施の形態１では、ＡＶコンテンツ送信装置１は、第２のＡＶコンテンツ受信装置３との間で互いに認証を行い、その認証が成功した場合に、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えるとした。しかしながら、ＡＶコンテンツ送信装置１は、第２のＡＶコンテンツ受信装置３からの認証要求を受信すると、認証が成功するか失敗するかにかかわらず、暗号化手法を拡張暗号化手法から基本暗号化手法に切り替えて、その切り替えた後の基本暗号化手法でＡＶコンテンツを暗号化して出力してもよい。ただしこの場合、ＡＶコンテンツ送信装置１と第２のＡＶコンテンツ受信装置３との間での認証が失敗すると、ＡＶコンテンツ送信装置１は、第２のＡＶコンテンツ受信装置３に交換鍵Ｋｅｘを出力しない。したがって、ＡＶコンテンツ送信装置１からのＡＶコンテンツは、不正な装置に解読されないように保護される。他方、ＡＶコンテンツ送信装置１が第２のコンテンツ受信装置３からの認証要求を受信して、暗号化手法を基本暗号化手法に切り替えて暗号化したＡＶコンテンツを出力する場合、上述した実施の形態１で説明したとおり、第１のコンテンツ受信装置２は、ＡＶコンテンツ送信装置１からの、暗号化手

法が基本暗号化手法に切り替わるという情報を入力し、ＡＶコンテンツ送信装置１からの基本暗号化手法で暗号化されたＡＶコンテンツを入力して、基本暗号化手法でそのＡＶコンテンツを解読することになる。一方その後、ＡＶコンテンツ送信装置１は、第２のコンテンツ受信装置３が不正であると判断した時点で、拡張暗号化手法に再変更する。

【００９１】さらに、請求項１０の本発明は、請求項１から９のいずれかに記載のＡＶコンテンツ送信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体である。また、請求項１３の本発明は、請求項１１または１２記載のＡＶコンテンツ受信方法の各ステップの全部または一部を実現するためのプログラムを格納したことを特徴とする媒体である。

【００９２】

【発明の効果】以上説明したところから明らかなように、本発明は、ＡＶコンテンツ送信装置が第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法を提供することができる。

【００９３】また、本発明は、第１の暗号化手法で暗号化したＡＶコンテンツを送信しているときに、その第１の暗号化手法を使用することができないＡＶコンテンツ受信装置がそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信装置を提供することができる。

【００９４】また、本発明は、上述したＡＶコンテンツ送信方法を用いたさい、第１の暗号化手法で暗号化されたＡＶコンテンツを受信し解読していた、第１の暗号化手法を使用することができないＡＶコンテンツ受信装置とは別のＡＶコンテンツ受信装置がある場合、その別のＡＶコンテンツ受信装置が引き続きそのＡＶコンテンツを解読することができるようにするＡＶコンテンツ送信方法およびＡＶコンテンツ受信方法を提供することができる。

【００９５】さらに、本発明は、上述したＡＶコンテンツ送信装置が第１の暗号化手法を使用することができないＡＶコンテンツ受信装置にそのＡＶコンテンツを解読させる場合、そのＡＶコンテンツ受信装置とは別に、第１の暗号化手法で暗号化されていたＡＶコンテンツを引き続き解読するＡＶコンテンツ受信装置を提供することができる。

＊【図面の簡単な説明】

【図１】本発明の実施の形態１のＡＶコンテンツ通信システムのブロック図

【図２】本発明の実施の形態１のＡＶコンテンツ通信システムのＡＶコンテンツ送信装置１が送信するＡＶコンテンツおよびコマンドを含むデータの構成図

【図３】本発明の実施の形態１のＡＶコンテンツ通信システムのＡＶコンテンツ送信装置１の動作の一部を示すフローチャート

【図４】本発明の実施の形態１のＡＶコンテンツ通信システムの第１のＡＶコンテンツ受信装置２の動作の一部を示すフローチャート

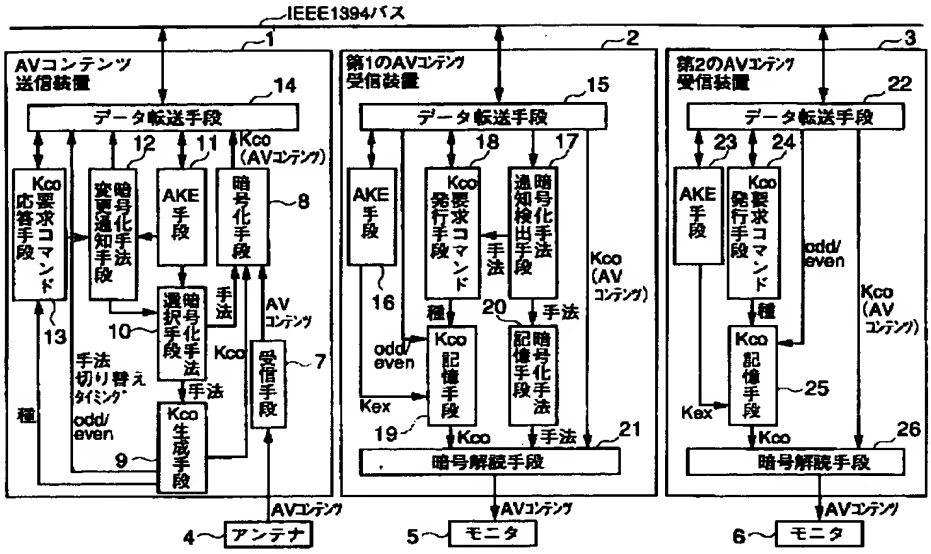
【図５】図３とは異なる、本発明の実施の形態１のＡＶコンテンツ通信システムのＡＶコンテンツ送信装置１の動作の一部を示すフローチャート

【図６】本発明の課題を説明するための図

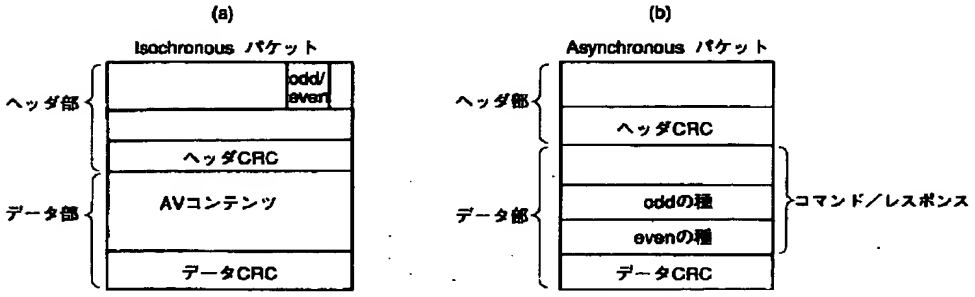
【符号の説明】

１　ＡＶコンテンツ送信装置
２　第１のＡＶコンテンツ受信装置
３　第２のＡＶコンテンツ受信装置
４　アンテナ
５、６　モニタ
７　受信手段
８　暗号化手段
９　Ｋｃｏ生成手段
１０　暗号化手法選択手段
１１　ＡＫＥ手段
１２　暗号化手法変更通知手段
１３　Ｋｃｏ要求コマンド応答手段
１４　データ転送手段
１５　データ転送手段
１６　ＡＫＥ手段
１７　暗号化手法通知検出手段
１８　Ｋｃｏ要求コマンド発行手段
１９　Ｋｃｏ記憶手段
２０　暗号化手法記憶手段
２１　暗号解読手段
２２　データ転送手段
２３　ＡＫＥ手段
２４　Ｋｃｏ要求コマンド発行手段
２５　Ｋｃｏ記憶手段
２６　暗号解読手段
２７　送信装置
２８　パソコン
２９　セットトップボックス（衛星放送受信機）

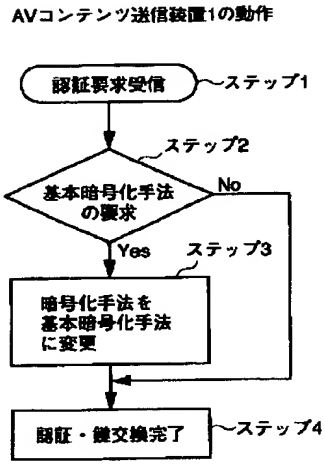
【図１】


IEEE1394バス
AVコンテンツ送信装置
第1のAVコンテンツ受信装置
第2のAVコンテンツ受信装置
データ転送手段
Kco要求応答手段
暗号化手法変更通知手段
AKE手段
暗号化手段
暗号化手法選択手段
Kco生成手段
受信手段
Kco要求コマンド発行手段
暗号化手法通知検出手段
Kco記憶手段
暗号化手法記憶手段
暗号解読手段
Kco要求コマンド
Kco記憶手段
暗号解読手段
Kco (AVコンテンツ)
AVコンテンツ
手法
種
Kex
odd/even
手法切り替えタイミング
アンテナ
モニタ
モニタ

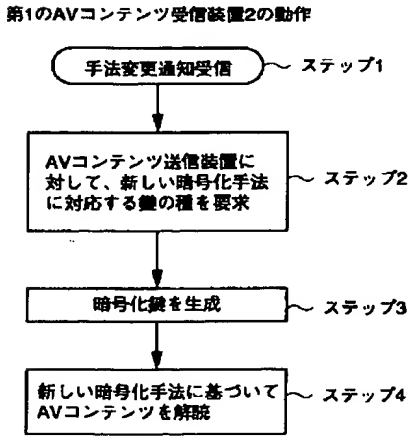
【図２】


(a)
Isochronous パケット
ヘッダ部
データ部
odd/even
ヘッダCRC
AVコンテンツ
データCRC
(b)
Asynchronous パケット
ヘッダ部
データ部
ヘッダCRC
oddの種
evenの種
データCRC
コマンド／レスポンス

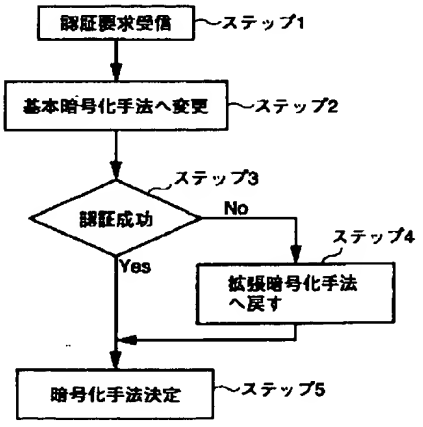
【図３】


AVコンテンツ送信装置1の動作
認証要求受信
ステップ1
ステップ2
基本暗号化手法の要求
No
Yes
ステップ3
暗号化手法を基本暗号化手法に変更
認証・鍵交換完了
ステップ4

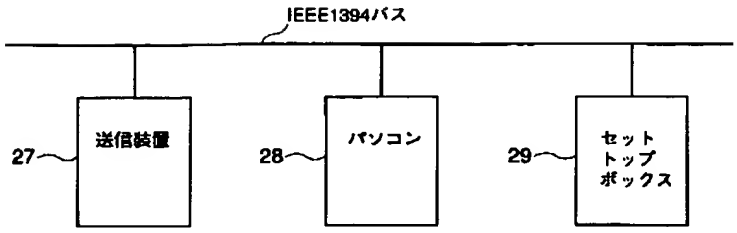
【図４】


第1のAVコンテンツ受信装置2の動作
手法変更通知受信
ステップ1
AVコンテンツ送信装置に対して、新しい暗号化手法に対応する鍵の種を要求
ステップ2
暗号化鍵を生成
ステップ3
新しい暗号化手法に基づいてAVコンテンツを解読
ステップ4

【図５】


認証要求受信
ステップ1
基本暗号化手法へ変更
ステップ2
ステップ3
認証成功
No
Yes
ステップ4
拡張暗号化手法へ戻す
暗号化手法決定
ステップ5

【図６】



フロントページの続き

(51) Int. Cl.[6]		識別記号	FI		
	Ｈ０４Ｌ	29/08	Ｈ０４Ｌ	9/00	６７３Ｂ
	Ｈ０４Ｎ	7/167		13/00	３０７Ｚ
//	Ｇ０６Ｆ	13/38	Ｈ０４Ｎ	7/167	Ｚ
	Ｈ０４Ｌ	12/28	Ｈ０４Ｌ	11/00	３１０Ｄ

(72)発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内